IN THE CLAIMS

Amend the claims as shown below by the markings.

1. (currently amended) A method of [[for]] logging a new user into a data processing device with an operating system and an accessible element ~~that is at least one of an application program and sensitive data~~, comprising the steps of:

ending a first user's access to the accessible element without unloading or restarting the accessible element, the accessible element being at least one of an application program and sensitive data;

determining authentication data for authenticating a second user;

defining an identity and access rights depending on the authentication data for the second user; and

providing access, depending on the defined access rights, to ~~for at [sic: "at" should be removed"]~~ the accessible element, that has not been unloaded or restarted, by the second user; and

sharing a same context ~~instance~~ of the accessible element between the first user and the second user without unloading or restarting the accessible element.

2. (original) The method according to claim 1, further comprising:

displaying a user interface, depending on the defined access rights;

performing a user switch process step that causes the method to begin again at the first step, content of a user interface remaining unchanged until access rights have been defined again.

3. (original) The method according to claim 2, wherein the content of the user interface is reduced if the renewed definition of access rights defines a more limited scope than the previous definition allowed.

4. (original) The method according to claim 3, further comprising:

generating a warning message indicating a reduction in content and that the user has an opportunity to begin the method at the first step again before the reduction.

5. (original) The method according to claim 1, further comprising:
displaying a user interface in accordance with the access rights that are defined;
deleting, by a User Logout procedure, content of a user interface; and
starting the method from the first step again.

6. (original) The method according to claim 1, further comprising:
logging all access to the application program and all access to the sensitive data together with the respectively defined identity.

7. (original) The method according to claim 1, further comprising:
activating a screen saver by a defined condition to make a user interface illegible; and
beginning the method from the first step again.

8. (original) The method according to claim 7, wherein the defined condition is some amount of elapsed time.

9. (original) The method according to claim 1, further comprising:
blocking all access rights based upon a failed attempt to authenticate a user in the first step.

10. (currently amended) A computer system, comprising:
a computer having a data storage media;
an accessible element that is at least one of an application program and sensitive data that is accessible by a first user and a same context ~~instance~~ of the accessible element that is accessible by a subsequent second user without unloading or restarting the accessible element;
a program stored in a memory element of the computer memory comprising:

a software module or algorithm configured to determine ~~for determining~~ authentication data for authenticating the second user with respect to the accessible element;

a software module or algorithm configured to define ~~for defining~~ an identity and access rights depending on the authentication data; and

a software module or algorithm configured to provide ~~for providing~~ access, depending on the defined access rights, for the accessible element without unloading or restarting the accessible element.

11. (currently amended) A data storage media having a program thereon that comprises:

a software module or algorithm configured to determine ~~for determining~~ authentication data for authenticating a user into a data processing device with an operating system and an accessible element that is at least one of an application program and sensitive data;

a software module or algorithm configured to define ~~for defining~~ an identity and access rights depending on the authentication data; and

a software module or algorithm configured to provide ~~for providing~~ access by the user, depending on the defined access rights, for a same context ~~instance~~ of the accessible element subsequent to an access of the accessible element by a prior first user without unloading or restarting the accessible element.